(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 107147648 A
(43)申请公布日 2017.09.08

(21)申请号 201710330977.3

(22)申请日 2017.05.11

(71)申请人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)

(72)发明人 郑劲松 郭涛

(74)专利代理机构 北京中强智尚知识产权代理有限公司 11448
代理人 王书彪 刘艳芬

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

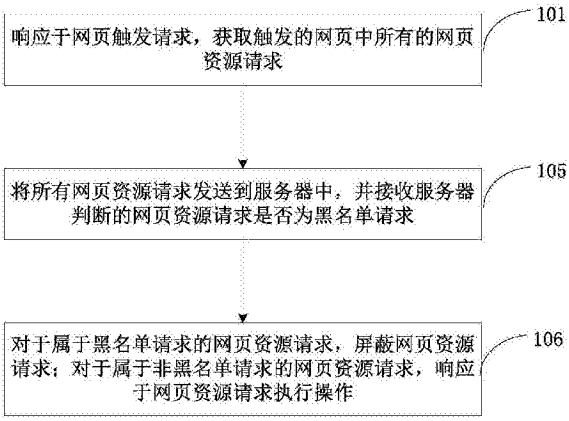
权利要求书2页 说明书12页 附图4页

(54)发明名称

资源请求的处理方法、客户端、服务器和系统

(57)摘要

本发明实施例公开了一种资源请求的处理方法、客户端、服务器和系统，其中，方法包括：响应于网页触发请求，获取触发的网页中所有的网页资源请求；将所有网页资源请求发送到服务器中，并接收服务器判断的网页资源请求是否为黑名单请求；对于属于黑名单请求的网页资源请求，屏蔽网页资源请求；对于属于非黑名单请求的网页资源请求，响应于网页资源请求执行操作。本发明实施例通过获取的所有网页资源请求发送到服务器中，并根据服务器发送的判断网页资源请求是否是黑名单请求执行操作，对黑名单请求进行屏蔽，有效拦截了对当前网页的流量注入；对于非黑名单请求，响应于该网页资源请求执行操作，在拦截流量注入的同时，保证了正常请求的操作。



CN 107147648 A

1.一种资源请求的处理方法,其特征在于,应用于客户端,包括:

响应于网页触发请求,获取所述触发的网页中所有的网页资源请求;

将所有网页资源请求发送到服务器中,并接收服务器判断的所述网页资源请求是否为黑名单请求;

对于属于黑名单请求的网页资源请求,屏蔽所述网页资源请求;

对于属于非黑名单请求的网页资源请求,响应于所述网页资源请求执行操作。

2.根据权利要求1所述的方法,其特征在于,所述获取所述触发的网页中所有的网页资源请求,包括:

遍历所述触发的网页对应的dom文档对象模型树,获取所述触发的网页中的所有url统一资源定位符,基于所述url统一资源定位符获得对应的网页资源请求。

3.根据权利要求1或2所述的方法,其特征在于,所述将所有网页资源请求发送到服务器中之前,还包括:

获取与所有所述网页资源请求对应的url统一资源定位符;判断所述url统一资源定位符与所述触发的网页对应的url是否为同源url;

将获得的非同源url对应的网页资源请求发送到服务器中;

对同源url对应的网页资源请求,响应于所述网页资源请求执行操作。

4.根据权利要求3所述的方法,其特征在于,所述获取与所述网页资源请求对应的url之后,包括:

若确定所述url中不包括所述客户端的网关地址,则响应于所述网页资源请求执行操作。

5.根据权利要求1至4任意一项所述的方法,其特征在于,所述屏蔽所述网页资源请求,包括:

操作所述触发的网页对应dom文档对象模型树对所述网页资源请求对应的url统一资源定位符进行屏蔽,通过屏蔽所述网页资源请求对应的url统一资源定位符实现屏蔽所述网页资源请求。

6.一种资源请求的处理方法,其特征在于,应用于服务器端,包括:

接收客户端发送的所有网页资源请求;

获取与所有所述网页资源请求对应的url统一资源定位符;

基于预存的数据判断所述url统一资源定位符是否为黑名单url将所述黑名单url对应的网页资源请求作为黑名单请求,将所述非黑名单url对应的网页资源请求作为非黑名单请求;

将所述网页资源请求是黑名单请求和/或是非黑名单请求发送给客户端。

7.根据权利要求6所述的方法,其特征在于,所述基于预存的数据判断所述url统一资源定位符是否为黑名单url,包括:

将所述url统一资源定位符与白名单数据库中预存的所有白名单url进行匹配;其中,所述白名单数据库中预存有所有白名单url;

对于存在匹配的白名单url的所述url对应的网页资源请求,输出判定所述网页资源请求属于非黑名单请求给客户端。

8.一种客户端,其特征在于,包括:

请求获取单元，用于响应于网页触发请求，获取所述触发的网页中所有的网页资源请求；

请求发送单元，用于将所有网页资源请求发送到服务器中，并接收服务器判断的所述网页资源请求是否为黑名单请求；

请求屏蔽单元，用于对于属于黑名单请求的网页资源请求，屏蔽所述网页资源请求；

请求响应单元，用于对于属于非黑名单请求的网页资源请求，响应于所述网页资源请求执行操作。

9.一种服务器，其特征在于，包括：

请求接收单元，用于接收客户端发送的所有网页资源请求；

获取单元，用于获取与所有所述网页资源请求对应的url统一资源定位符；

黑名单判断单元，用于基于预存的数据判断所述url统一资源定位符是否为黑名单url，将所述黑名单url对应的网页资源请求作为黑名单请求，将所述非黑名单url对应的网页资源请求作为非黑名单请求，并将判断结果发送到结果发送单元；

结果发送单元，用于将黑名单判断单元发送的判断结果发送给客户端。

10.一种资源请求的处理系统，其特征在于，包括如权利要求9所述的服务器和至少一个如权利要求8所述的客户端。

资源请求的处理方法、客户端、服务器和系统

技术领域

[0001] 本发明涉及网络资源处理技术，尤其是一种资源请求的处理方法、客户端、服务器和系统。

背景技术

[0002] 随着互联网技术的迅猛发展，人们的很多生活行为都在网络上完成，如通讯、购物等等。正因如此各种钓鱼行为也在威胁广大网民的信息安全以及财产安全。

[0003] 之前大多数的钓鱼欺诈行为是通过恶意的黑网站的来进行的，当用户访问该黑网站时，个人信息安全、财产安全等会受到威胁。

[0004] 恶意网站，例如钓鱼网站、或者是欺诈，仿冒网站等，主要是通过仿冒真实网站的URL地址或是页面内容，伪装成银行及电子商务等类型的网站，或是利用真实网站服务器程序上的漏洞，在该网站的某些网页中插入危险的网页代码，以此来骗取用户银行或信用卡账号、密码等私人资料。恶意网页中包含着许多敏感的特征，例如，金融欺诈类的恶意网页会在文字、图片等方面仿冒官网，或是在真实网页中插入虚假票务、虚假中奖、假冒网银、虚假购物等信息，这些特征大多以文本串的形式出现在网页中。

[0005] 现有的为了防范恶意网站的主要手段是当用户访问某网站时，客户端将网站的URL发送至服务器端的黑白名单数据库进行查询，所谓的黑名单数据库即是已审核确认的恶意网站的URL名单数据库，所谓的白名单数据库即是已审核确认的安全网站的URL。服务器端经过查询后，将网站是否属于恶意网站的结果反馈给客户端。

发明内容

[0006] 本发明实施例所要解决的一个技术问题是：提供一种自动识别恶意请求并进行屏蔽的资源请求的处理技术。

[0007] 本发明实施例提供的一种资源请求的处理方法，应用于客户端，包括：

[0008] 响应于网页触发请求，获取所述触发的网页中所有的网页资源请求；

[0009] 将所有网页资源请求发送到服务器中，并接收服务器判断的所述网页资源请求是否为黑名单请求；

[0010] 对于属于黑名单请求的网页资源请求，屏蔽所述网页资源请求；

[0011] 对于属于非黑名单请求的网页资源请求，响应于所述网页资源请求执行操作。

[0012] 基于上述方法的另一实施例中，所述获取所述触发的网页中所有的网页资源请求，包括：

[0013] 遍历所述触发的网页对应的dom文档对象模型树，获取所述触发的网页中的所有url统一资源定位符，基于所述url统一资源定位符获得对应的网页资源请求。

[0014] 基于上述方法的另一实施例中，所述将所有网页资源请求发送到服务器中之前，还包括：

[0015] 获取与所有所述网页资源请求对应的url统一资源定位符；判断所述url统一资源

定位符与所述触发的网页对应的url是否为同源url；

[0016] 将获得的非同源url对应的网页资源请求发送到服务器中；

[0017] 对同源url对应的网页资源请求，响应于所述网页资源请求执行操作。

[0018] 基于上述方法的另一实施例中，所述获取与所述网页资源请求对应的url之后，包括：

[0019] 若确定所述url中不包括所述客户端的网关地址，则响应于所述网页资源请求执行操作。

[0020] 基于上述方法的另一实施例中，所述屏蔽所述网页资源请求，包括：

[0021] 操作所述触发的网页对应dom文档对象模型树对所述网页资源请求对应的url统一资源定位符进行屏蔽，通过屏蔽所述网页资源请求对应的url统一资源定位符实现屏蔽所述网页资源请求。

[0022] 根据本发明实施例的另一个方面，提供的一种资源请求的处理方法，应用于服务器端，包括：

[0023] 接收客户端发送的所有网页资源请求；

[0024] 获取与所有所述网页资源请求对应的url统一资源定位符；

[0025] 基于预存的数据判断所述url统一资源定位符是否为黑名单url，将黑名单url对应的网页资源请求作为黑名单请求，将非黑名单url对应的网页资源请求作为非黑名单请求；

[0026] 将所述网页资源请求是黑名单请求和/或是非黑名单请求发送给客户端。

[0027] 根据本发明实施例的另一个方面，提供的一种客户端，包括：

[0028] 请求获取单元，用于响应于网页触发请求，获取所述触发的网页中所有的网页资源请求；

[0029] 请求发送单元，用于将所有网页资源请求发送到服务器中，并接收服务器判断的所述网页资源请求是否为黑名单请求；

[0030] 请求屏蔽单元，用于对于属于黑名单请求的网页资源请求，屏蔽所述网页资源请求；

[0031] 请求响应单元，用于对于属于非黑名单请求的网页资源请求，响应于所述网页资源请求执行操作。

[0032] 根据本发明实施例的另一个方面，提供的一种服务器，包括：

[0033] 请求接收单元，用于接收客户端发送的所有网页资源请求；

[0034] 获取单元，用于获取与所有所述网页资源请求对应的url统一资源定位符；

[0035] 黑名单判断单元，用于基于预存的数据判断所述url统一资源定位符是否为黑名单url，将所述黑名单url对应的网页资源请求作为黑名单请求，将所述非黑名单url对应的网页资源请求作为非黑名单请求，并将判断结果发送到结果发送单元；

[0036] 结果发送单元，用于将黑名单判断单元发送的判断结果发送给客户端。

[0037] 根据本发明实施例的另一个方面，提供的一种资源请求的处理系统，包括如上所述的服务器和至少一个如上所述的客户端。

[0038] 基于本发明上述实施例提供的一种资源请求的处理方法、客户端、服务器和系统，通过获取的所有网页资源请求发送到服务器中，并根据服务器发送的判断网页资源请求是

否是黑名单请求执行操作，对黑名单请求进行屏蔽，有效拦截了对当前网页的流量注入；对于非黑名单请求，响应于该网页资源请求执行操作，在拦截流量注入的同时，保证了正常请求的操作。

[0039] 下面通过附图和实施例，对本发明的技术方案做进一步的详细描述。

附图说明

[0040] 构成说明书的一部分的附图描述了本发明的实施例，并且连同描述一起用于解释本发明的原理。

[0041] 参照附图，根据下面的详细描述，可以更加清楚地理解本发明，其中：

[0042] 图1为本发明资源请求的处理方法一个实施例的流程图。

[0043] 图2为本发明资源请求的处理方法另一个实施例的流程图。

[0044] 图3为本发明客户端一个实施例的结构示意图。

[0045] 图4为本发明客户端另一个实施例的结构示意图。

[0046] 图5为本发明资源请求的处理方法一个实施例的流程图。

[0047] 图6为本发明服务器一个实施例的结构示意图。

[0048] 图7为本发明服务器另一个实施例的结构示意图。

具体实施方式

[0049] 现在将参照附图来详细描述本发明的各种示例性实施例。应注意到：除非另外具体说明，否则在这些实施例中阐述的部件和步骤的相对布置、数字表达式和数值不限制本发明的范围。

[0050] 同时，应当明白，为了便于描述，附图中所示出的各个部分的尺寸并不是按照实际的比例关系绘制的。

[0051] 以下对至少一个示例性实施例的描述实际上仅仅是说明性的，决不作为对本发明及其应用或使用的任何限制。

[0052] 对于相关领域普通技术人员已知的技术、方法和设备可能不作详细讨论，但在适当情况下，所述技术、方法和设备应当被视为说明书的一部分。

[0053] 应注意到：相似的标号和字母在下面的附图中表示类似项，因此，一旦某一项在一个附图中被定义，则在随后的附图中不需要对其进行进一步讨论。

[0054] 本发明实施例可以应用于计算机系统/服务器，其可与众多其它通用或专用计算系统环境或配置一起操作。适于与计算机系统/服务器一起使用的众所周知的计算系统、环境和/或配置的例子包括但不限于：个人计算机系统、服务器计算机系统、瘦客户机、厚客户机、手持或膝上设备、基于微处理器的系统、机顶盒、可编程消费电子产品、网络个人电脑、小型计算机系统、大型计算机系统和包括上述任何系统的分布式云计算技术环境，等等。

[0055] 计算机系统/服务器可以在由计算机系统执行的计算机系统可执行指令(诸如程序模块)的一般语境下描述。通常，程序模块可以包括例程、程序、目标程序、组件、逻辑、数据结构等等，它们执行特定的任务或者实现特定的抽象数据类型。计算机系统/服务器可以在分布式云计算环境中实施，分布式云计算环境中，任务是由通过通信网络链接的远程处理设备执行的。在分布式云计算环境中，程序模块可以位于包括存储设备的本地或远程计

算系统存储介质上。

[0056] 图1为本发明资源请求的处理方法一个实施例的流程图。如图1所示，该方法应用于客户端，该实施例方法包括：

[0057] 步骤101，响应于网页触发请求，获取触发的网页中所有的网页资源请求。

[0058] 具体实现过程可以是，在客户端中中打开某一浏览器(对浏览器的种类并不限定)，通过该浏览器接收到网页触发请求，根据该网页触发请求打开网页后，遍历网页中所有的url统一资源定位符，就可以获得所请求网页中所有的网页资源请求，其中，网页资源请求指对网络资源存在占用问题和/或对所请求网页注入流量的请求。

[0059] 步骤105，将所有网页资源请求发送到服务器中，并接收服务器判断的网页资源请求是否为黑名单请求。

[0060] 本申请目前提出的方案中对于黑名单的判断是在服务器中完成的，该服务器和客户端可以属于同一网络，或属于不同网络。

[0061] 步骤106，对于属于黑名单请求的网页资源请求，屏蔽网页资源请求；对于属于非黑名单请求的网页资源请求，响应于网页资源请求执行操作。

[0062] 基于本发明上述实施例提供的资源请求的处理方法，通过获取的所有网页资源请求发送到服务器中，并根据服务器发送的判断网页资源请求是否是黑名单请求执行操作，对黑名单请求进行屏蔽，有效拦截了对当前网页的流量注入；对于非黑名单请求，响应于该网页资源请求执行操作，在拦截流量注入的同时，保证了正常请求的操作。

[0063] 在本发明资源请求的处理方法上述实施例的一个具体示例中，步骤101具体还可以包括：

[0064] 遍历触发的网页对应的dom文档对象模型树，获取触发的网页中的所有url统一资源定位符，基于url统一资源定位符获得对应的网页资源请求。

[0065] 在本实施例中，将触发的网页解析成dom树，解析的方法包括但不限于以下几种方式：

[0066] 第一种方法，WebBrowser控件会将所有的页面元素全部下载下来，比较慢，若没有下载完，相关的UI属性不是最后网页所展现的样式；这种方法，解析网页很慢，但是分析网页非常详尽；

[0067] 第二种方法比第一种方法快，而且也可以取到UI属性；不同的是，源码下载这一块可以自己单独控制，但是，对于有iframe框架的网页，推荐用第一种方法来解析；

[0068] 第三种方法解析后的dom树没有ui属性；但是解析速度非常快；只是需要操作单独的元素，也就够了，但是，有内存泄漏，要求不很严格的情况下，可以使用下。

[0069] 遍历解析触发的网页获得的dom树，获得所有的url，url为统一资源定位符是对可以从互联网上得到的资源的位置和访问方法的一种简洁的表示，是互联网上标准资源的地址。互联网上的每个文件都有一个唯一的url，它包含的信息指出文件的位置以及浏览器应该怎么处理它。由于url的特性，基于获得的url就可以获得对应该url的网页资源请求。

[0070] 图2为本发明资源请求的处理方法另一个实施例的流程图。在上述各实施例的基础上，如图2所示，本实施例方法包括：

[0071] 步骤101，响应于网页触发请求，获取触发的网页中所有的网页资源请求。

[0072] 步骤202，获取与所有网页资源请求对应的url统一资源定位符；

[0073] 步骤203，判断url统一资源定位符与触发的网页对应的url是否为同源url，如果是，执行步骤204；否则，执行步骤105。

[0074] 步骤204，对同源url对应的网页资源请求，响应于网页资源请求执行操作。

[0075] 步骤105，将所有网页资源请求发送到服务器中，并接收服务器判断的网页资源请求是否为黑名单请求。

[0076] 此时发送到服务器中的网页资源请求是获得的非同源url对应的网页资源请求。

[0077] 步骤106，对于属于黑名单请求的网页资源请求，屏蔽网页资源请求；对于属于非黑名单请求的网页资源请求，响应于网页资源请求执行操作。

[0078] 本实施例中对网页资源请求对应的url统一资源定位符与所触发的网页的url统一资源定位符进行比对，就可以判断是否同源，同源是指两个网页的协议、域名和端口都相同，通常一个网页自身内置的链接网址都是与该网页同源的，所以，当判断网页资源请求对应的url与触发网页的url是同源时，可默认该网页资源请求是正常请求，响应该网页资源请求执行操作，只有当判断该网页资源请求与所触发网页是非同源时，才需要将网页资源请求发送给服务器进行鉴别。

[0079] 在本发明方法上述实施例的一个具体示例中，步骤202与步骤203之间还包括：

[0080] 若确定url中不包括客户端的网关地址，则响应于网页资源请求执行操作。

[0081] 当网页资源请求对应的url中不包括当前客户端的网关地址时，可以直接证明所获取的域名解析地址没有被篡改；若所述统一资源定位符中包括所述用户设备的网关地址，且所述统一资源定位符中还包括路由器的配置参数，则获取所述路由器的配置参数中包括的域名解析地址；举例来说，假设上述URL中包括的被请求的网页所在的服务器地址(例如192.168.1.1)与用户设备的网关地址(例如192.168.1.1)是一致的，而且上述URL中还包括路由器的配置参数，则获取路由器的配置参数包括的域名解析地址，例如dns server＝106.186.29.231，或dns server2＝114.114.114.114。

[0082] 本发明资源请求的处理方法的又一个实施例中，在上述各实施例的基础上，步骤106中屏蔽网页资源请求的过程可以包括：

[0083] 操作触发的网页对应dom文档对象模型树对网页资源请求对应的url统一资源定位符进行屏蔽，通过屏蔽网页资源请求对应的url统一资源定位符实现屏蔽网页资源请求。

[0084] 本实施例中，通过对触发的网页解析获得的dom树执行操作，对判定位黑名单请求的网页资源请求对应的url执行屏蔽，以实现对是黑名单请求的网页资源请求屏蔽，其中涉及的通过dom树对某些url进行屏蔽的技术属于现有技术，在此不赘述。

[0085] 本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0086] 图3为本发明客户端一个实施例的结构示意图。该实施例的客户端可用于实现本发明上述各方法实施例。如图3所示，该实施例的客户端包括：

[0087] 请求获取单元31，用于响应于网页触发请求，获取触发的网页中所有的网页资源请求。

[0088] 请求发送单元34，用于将所有网页资源请求发送到服务器中，并接收服务器判断

的网页资源请求是否为黑名单请求。

[0089] 请求屏蔽单元35，用于对于属于黑名单请求的网页资源请求，屏蔽网页资源请求。

[0090] 请求响应单元36，用于对于属于非黑名单请求的网页资源请求，响应于网页资源请求执行操作。

[0091] 基于本发明上述实施例提供的一种客户端，通过获取的所有网页资源请求发送到服务器中，并根据服务器发送的判断网页资源请求是否是黑名单请求执行操作，对黑名单请求进行屏蔽，有效拦截了对当前网页的流量注入；对于非黑名单请求，响应于该网页资源请求执行操作，在拦截流量注入的同时，保证了正常请求的操作。

[0092] 在本发明客户端上述实施例的一个具体示例中，请求获取单元31，具体用于遍历触发的网页对应的dom文档对象模型树，获取触发的网页中的所有url统一资源定位符，基于url统一资源定位符获得对应的网页资源请求。

[0093] 图4为本发明客户端另一个实施例的结构示意图。在上述实施例的基础上，在请求获取单元31和请求发送单元34之间，还包括：

[0094] url获取单元42，用于获取与所有网页资源请求对应的url统一资源定位符。

[0095] 同源判断单元43，用于判断url统一资源定位符与触发的网页对应的url是否为同源url；将获得的非同源url对应的网页资源请求发送到服务器中；对同源url对应的网页资源请求，响应于网页资源请求执行操作。

[0096] 本实施例中对网页资源请求对应的url统一资源定位符与所触发的网页的url统一资源定位符进行比对，就可以判断是否同源，同源是指两个网页的协议、域名和端口都相同，通常一个网页自身内置的链接网址都是与该网页同源的，所以，当判断网页资源请求对应的url与触发网页的url是同源时，可默认该网页资源请求是正常请求，响应该网页资源请求执行操作，只有当判断该网页资源请求与所触发网页是非同源时，才需要将网页资源请求发送给服务器进行鉴别。

[0097] 在本发明客户端上述实施例的一个具体示例中，在url获取单元42和同源判断单元43之间还可以包括：

[0098] url判定单元，用于若确定url中不包括客户端的网关地址，则响应于所述网页资源请求执行操作。

[0099] 本发明客户端的又一个实施例中，在上述各实施例的基础上，请求屏蔽单元35，具体用于操作触发的网页对应dom文档对象模型树对网页资源请求对应的url统一资源定位符进行屏蔽，通过屏蔽网页资源请求对应的url统一资源定位符实现屏蔽网页资源请求。

[0100] 本实施例中，通过对触发的网页解析获得的dom树执行操作，对判定位黑名单请求的网页资源请求对应的url执行屏蔽，以实现对是黑名单请求的网页资源请求屏蔽，其中涉及的通过dom树对某些url进行屏蔽的技术属于现有技术，在此不赘述。

[0101] 图5为本发明资源请求的处理方法一个实施例的流程图。如图5所示，该方法应用于服务器，该实施例方法包括：

[0102] 步骤501，接收客户端发送的所有网页资源请求。

[0103] 步骤502，获取与所有网页资源请求对应的url统一资源定位符。

[0104] 由于客户端获取网页资源请求时是通过url统一资源定位符获取的，因此，客户端将网页资源请求发送给服务器时，可以同时将所有网页资源请求对应的url发送给服务器，

此时服务器将直接获取到url;还有一种可能是,客户端未将url与网页资源请求一同发送给服务器,此时,服务器需要通过网页资源请求获取对应的url。

[0105] 步骤503,基于预存的数据判断url统一资源定位符是否为黑名单url,将黑名单url对应的网页资源请求作为黑名单请求,将非黑名单url对应的网页资源请求作为非黑名单请求。

[0106] 步骤504,将网页资源请求是黑名单请求和/或是非黑名单请求发送给客户端。

[0107] 基于本发明上述实施例提供的一种资源请求的处理方法,服务器对从客户端发送来的网页资源请求,首先获取网页资源请求对应的url,并根据获得的url判断其是否是黑名单url,将是黑名单url的url对应的网页资源请求作为黑名单请求发送给客户端,将非黑名单url对应的网页资源请求作为非黑名单请求发送给客户端,该方法通过url基于黑名单url完成了初级判断,将存储在服务器中已知是黑名单url的url筛选出,并且服务器由于与多个客户端相连接,因此,其中存储的黑名单url相对单独的客户端更全面,判断出的黑名单结果更具可信度。

[0108] 本发明资源请求的处理方法的另一个实施例中,在上述实施例的基础上,步骤503判断url统一资源定位符是否为黑名单url过程,具体可以包括:

[0109] 将url统一资源定位符与白名单数据库中预存的所有白名单url进行匹配;其中,白名单数据库中预存有所有白名单url;

[0110] 对于存在匹配的白名单url的url对应的网页资源请求,输出判定所述网页资源请求属于非黑名单请求给客户端。

[0111] 对于url首先基于白名单数据库判断其是否为白名单url,白名单数据库中预存有所有白名单url;对于判断url是否为黑名单url是有一定的不确定性的,有些可能是存疑的,因此,为了客户端的安全性,首先将url与白名单数据库中的url进行匹配,白名单数据库中的url是确定的无害的url,因此,通过白名单数据库的匹配,输出的非黑名单url可以完全确保客户端的安全性。

[0112] 在本发明资源请求的处理方法上述各实施例的一个具体示例中,还包括:

[0113] 对于不存在匹配的白名单url的url进行量级筛选获得可疑url;

[0114] 若url中包括路由器的配置参数,则获取路由器的配置参数中包括的域名解析地址;

[0115] 查询黑名单库,确定域名解析地址包括在黑名单库中,则判断url为黑名单url;黑名单库中保存有云安全服务器预先收集的危险的域名解析地址。

[0116] 在本实施例中提出了对于不是白名单的url进行量级筛选,通常对于正常插入网页的请求应当是所有客户端都接收到的请求,而非法插入的网页资源请求多数内置在某个或某些客户端中的插件发出的,因此,非法网页资源请求在量级上与合法网页资源请求相比会小很多,因此,通过量级大小就可以在非白名单url中筛选得到可疑url。

[0117] 在本发明资源请求的处理方法上述各实施例的一个具体示例中,还包括:

[0118] 当url对应的域名解析地址不包括在所述黑名单库中时,判断统一资源定位符的refer链的地址是否为外网IP地址;

[0119] 若确定统一资源定位符的refer链的地址为外网IP地址,则屏蔽网页资源请求;

[0120] 若确定统一资源定位符的refer链的地址不是外网IP地址,则响应于所述网页资

源请求执行操作。

[0121] 本领域普通技术人员可以理解:实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成,前述的程序可以存储于一计算机可读取存储介质中,该程序在执行时,执行包括上述方法实施例的步骤;而前述的存储介质包括:ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0122] 图6为本发明服务器一个实施例的结构示意图。该实施例的服务器可用于实现本发明上述各方法实施例。如图6所示,该实施例服务器中,包括:

[0123] 请求接收单元61,用于接收客户端发送的所有网页资源请求。

[0124] 获取单元62,用于获取与所有网页资源请求对应的url统一资源定位符。

[0125] 黑名单判断单元63,用于基于预存的数据判断url统一资源定位符是否为黑名单url,将黑名单url对应的网页资源请求作为黑名单请求,将非黑名单url对应的网页资源请求作为非黑名单请求,并将判断结果发送到结果发送单元。

[0126] 结果发送单元64,用于将黑名单判断单元发送的判断结果发送给客户端。

[0127] 基于本发明上述实施例提供的一种服务器,服务器对从客户端发送来的网页资源请求,首先获取网页资源请求对应的url,并根据获得的url判断其是否是黑名单url,将是黑名单url的url对应的网页资源请求作为黑名单请求发送给客户端,将非黑名单url对应的网页资源请求作为非黑名单请求发送给客户端,该方法通过url基于黑名单url完成了初级判断,将存储在服务器中已知是黑名单url的url筛选出,并且服务器由于与多个客户端相连接,因此,其中存储的黑名单url相对单独的客户端更全面,判断出的黑名单结果更具可信度。

[0128] 图7为本发明服务器另一个实施例的结构示意图。在上述实施例的基础上,本实施例服务器中黑名单判断单元63包括:

[0129] 白名单匹配模块631,用于将url统一资源定位符与白名单数据库中预存的所有白名单url进行匹配,对存在匹配的白名单url的所述url对应的网页资源请求,判定为非黑名单请求给结果发送单元;其中,白名单数据库中预存有所有白名单url。

[0130] 对于url首先基于白名单数据库判断其是否为白名单url,白名单数据库中预存有所有白名单url;对于判断url是否为黑名单url是有一定的不确定性的,有些可能是存疑的,因此,为了客户端的安全性,首先将url与白名单数据库中的url进行匹配,白名单数据库中的url是确定的无害的url,因此,通过白名单数据库的匹配,输出的非黑名单url可以完全确保客户端的安全性。

[0131] 在本发明服务器上述各实施例的一个具体示例中,黑名单判断单元63还包括:

[0132] 筛选模块632,用于对于不存在匹配的白名单url的url进行量级筛选获得可疑url。

[0133] 解析模块633,用于当url中包括路由器的配置参数,则获取路由器的配置参数中包括的域名解析地址。

[0134] 库查询模块634,用于查询黑名单库,确定域名解析地址包括在黑名单库中,则判断url为黑名单url;黑名单库中保存有云安全服务器预先收集的危险的域名解析地址。

[0135] 在本发明服务器上述各实施例的一个具体示例中,库查询模块634,还用于当url对应的域名解析地址不包括在黑名单库中时,判断统一资源定位符的refer链的地址是否

为外网IP地址。

[0136] 黑名单判断单元63，还包括：

[0137] IP地址判断模块635，对确定url的refer链的地址为外网IP地址的，确定url对应的网页资源请求为黑名单请求；对确定url的refer链的地址不是外网IP地址，确定url对应的网页资源请求为非黑名单请求。

[0138] 根据本发明实施例的另一个方面，提供的一种资源请求的处理系统，包括如上述实施例中任意一项的服务器和至少一个如上述实施例中任意一项的客户端。

[0139] 1、一种资源请求的处理方法，应用于客户端，包括：

[0140] 响应于网页触发请求，获取所述触发的网页中所有的网页资源请求；

[0141] 将所有网页资源请求发送到服务器中，并接收服务器判断的所述网页资源请求是否为黑名单请求；

[0142] 对于属于黑名单请求的网页资源请求，屏蔽所述网页资源请求；

[0143] 对于属于非黑名单请求的网页资源请求，响应于所述网页资源请求执行操作。

[0144] 2、根据1所述的方法，所述获取所述触发的网页中所有的网页资源请求，包括：

[0145] 遍历所述触发的网页对应的dom文档对象模型树，获取所述触发的网页中的所有url统一资源定位符，基于所述url统一资源定位符获得对应的网页资源请求。

[0146] 3、根据1或2所述的方法，所述将所有网页资源请求发送到服务器中之前，还包括：

[0147] 获取与所有所述网页资源请求对应的url统一资源定位符；判断所述url统一资源定位符与所述触发的网页对应的url是否为同源url；

[0148] 将获得的非同源url对应的网页资源请求发送到服务器中；

[0149] 对同源url对应的网页资源请求，响应于所述网页资源请求执行操作。

[0150] 4、根据3所述的方法，所述获取与所述网页资源请求对应的url之后，包括：

[0151] 若确定所述url中不包括所述客户端的网关地址，则响应于所述网页资源请求执行操作。

[0152] 5、根据1至4任意一项所述的方法，所述屏蔽所述网页资源请求，包括：

[0153] 操作所述触发的网页对应dom文档对象模型树对所述网页资源请求对应的url统一资源定位符进行屏蔽，通过屏蔽所述网页资源请求对应的url统一资源定位符实现屏蔽所述网页资源请求。

[0154] 6、一种资源请求的处理方法，应用于服务器端，包括：

[0155] 接收客户端发送的所有网页资源请求；

[0156] 获取与所有所述网页资源请求对应的url统一资源定位符；

[0157] 基于预存的数据判断所述url统一资源定位符是否为黑名单url将所述黑名单url对应的网页资源请求作为黑名单请求，将所述非黑名单url对应的网页资源请求作为非黑名单请求；

[0158] 将所述网页资源请求是黑名单请求和/或是非黑名单请求发送给客户端。

[0159] 7、根据6所述的方法，所述基于预存的数据判断所述url统一资源定位符是否为黑名单url，包括：

[0160] 将所述url统一资源定位符与白名单数据库中预存的所有白名单url进行匹配；其中，所述白名单数据库中预存有所有白名单url；

[0161] 对于存在匹配的白名单url的所述url对应的网页资源请求，输出判定所述网页资源请求属于非黑名单请求给客户端。

[0162] 8、根据7所述的方法，还包括：

[0163] 对于不存在匹配的白名单url的所述url进行量级筛选获得可疑url；

[0164] 若所述url中包括路由器的配置参数，则获取所述路由器的配置参数中包括的域名解析地址；

[0165] 查询黑名单库，确定所述域名解析地址包括在所述黑名单库中，则判断所述url为黑名单url；所述黑名单库中保存有云安全服务器预先收集的危险的域名解析地址。

[0166] 9、根据8所述的方法，还包括：

[0167] 当所述url对应的所述域名解析地址不包括在所述黑名单库中时，判断所述统一资源定位符的refer链的地址是否为外网IP地址；

[0168] 若确定所述统一资源定位符的refer链的地址为外网IP地址，则屏蔽所述网页资源请求；

[0169] 若确定所述统一资源定位符的refer链的地址不是外网IP地址，则响应于所述网页资源请求执行操作。

[0170] 10、一种客户端，包括：

[0171] 请求获取单元，用于响应于网页触发请求，获取所述触发的网页中所有的网页资源请求；

[0172] 请求发送单元，用于将所有网页资源请求发送到服务器中，并接收服务器判断的所述网页资源请求是否为黑名单请求；

[0173] 请求屏蔽单元，用于对于属于黑名单请求的网页资源请求，屏蔽所述网页资源请求；

[0174] 请求响应单元，用于对于属于非黑名单请求的网页资源请求，响应于所述网页资源请求执行操作。

[0175] 11、根据10所述的客户端，所述请求获取单元，具体用于遍历所述触发的网页对应的dom文档对象模型树，获取所述触发的网页中的所有url统一资源定位符，基于所述url统一资源定位符获得对应的网页资源请求。

[0176] 12、根据10或11所述的客户端，还包括：

[0177] url获取单元，用于获取与所有所述网页资源请求对应的url统一资源定位符；

[0178] 同源判断单元，用于判断所述url统一资源定位符与所述触发的网页对应的url是否为同源url；将获得的非同源url对应的网页资源请求发送到服务器中；对同源url对应的网页资源请求，响应于所述网页资源请求执行操作。

[0179] 13、根据12所述的客户端，还包括：

[0180] url判定单元，用于若确定所述url中不包括所述客户端的网关地址，则响应于所述网页资源请求执行操作。

[0181] 14、根据10至13任意一项所述的客户端，所述请求屏蔽单元，具体用于操作所述触发的网页对应dom文档对象模型树对所述网页资源请求对应的url统一资源定位符进行屏蔽，通过屏蔽所述网页资源请求对应的url统一资源定位符实现屏蔽所述网页资源请求。

[0182] 15、一种服务器，包括：

[0183] 请求接收单元，用于接收客户端发送的所有网页资源请求；

[0184] 获取单元，用于获取与所有所述网页资源请求对应的url统一资源定位符；

[0185] 黑名单判断单元，用于基于预存的数据判断所述url统一资源定位符是否为黑名单url，将所述黑名单url对应的网页资源请求作为黑名单请求，将所述非黑名单url对应的网页资源请求作为非黑名单请求，并将判断结果发送到结果发送单元；

[0186] 结果发送单元，用于将黑名单判断单元发送的判断结果发送给客户端。

[0187] 16、根据15所述的服务器，所述黑名单判断单元包括：

[0188] 白名单匹配模块，用于将所述url统一资源定位符与白名单数据库中预存的所有白名单url进行匹配，对存在匹配的白名单url的所述url对应的网页资源请求，判定为非黑名单请求给结果发送单元；其中，所述白名单数据库中预存有所有白名单url。

[0189] 17、根据16所述的服务器，所述黑名单判断单元还包括：

[0190] 筛选模块，用于对于不存在匹配的白名单url的所述url进行量级筛选获得可疑url；

[0191] 解析模块，用于当所述url中包括路由器的配置参数，则获取所述路由器的配置参数中包括的域名解析地址；

[0192] 库查询模块，用于查询黑名单库，确定所述域名解析地址包括在所述黑名单库中，则判断所述url为黑名单url；所述黑名单库中保存有云安全服务器预先收集的危险的域名解析地址。

[0193] 18、根据17所述的服务器，库查询模块，还用于当所述url对应的所述域名解析地址不包括在所述黑名单库中时，判断所述统一资源定位符的refer链的地址是否为外网IP地址；

[0194] 所述黑名单判断单元，还包括：

[0195] IP地址判断模块，对确定所述url的refer链的地址为外网IP地址的，确定所述url对应的网页资源请求为黑名单请求；对确定所述url的refer链的地址不是外网IP地址，确定所述url对应的网页资源请求为非黑名单请求。

[0196] 19、一种资源请求的处理系统，包括如15至18任意一项所述的服务器和至少一个如10至14任意一项所述的客户端。

[0197] 本说明书中各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其它实施例的不同之处，各个实施例之间相同或相似的部分相互参见即可。对于系统实施例而言，由于其与方法实施例基本对应，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0198] 可能以许多方式来实现本发明的方法和装置。例如，可通过软件、硬件、固件或者软件、硬件、固件的任何组合来实现本发明的方法和装置。用于所述方法的步骤的上述顺序仅是为了进行说明，本发明的方法的步骤不限于以上具体描述的顺序，除非以其它方式特别说明。此外，在一些实施例中，还可将本发明实施为记录在记录介质中的程序，这些程序包括用于实现根据本发明的方法的机器可读指令。因而，本发明还覆盖存储用于执行根据本发明的方法的程序的记录介质。

[0199] 本发明的描述是为了示例和描述起见而给出的，而并不是无遗漏的或者将本发明限于所公开的形式。很多修改和变化对于本领域的普通技术人员而言是显然的。选择和描

述实施例是为了更好说明本发明的原理和实际应用，并且使本领域的普通技术人员能够理解本发明从而设计适于特定用途的带有各种修改的各种实施例。

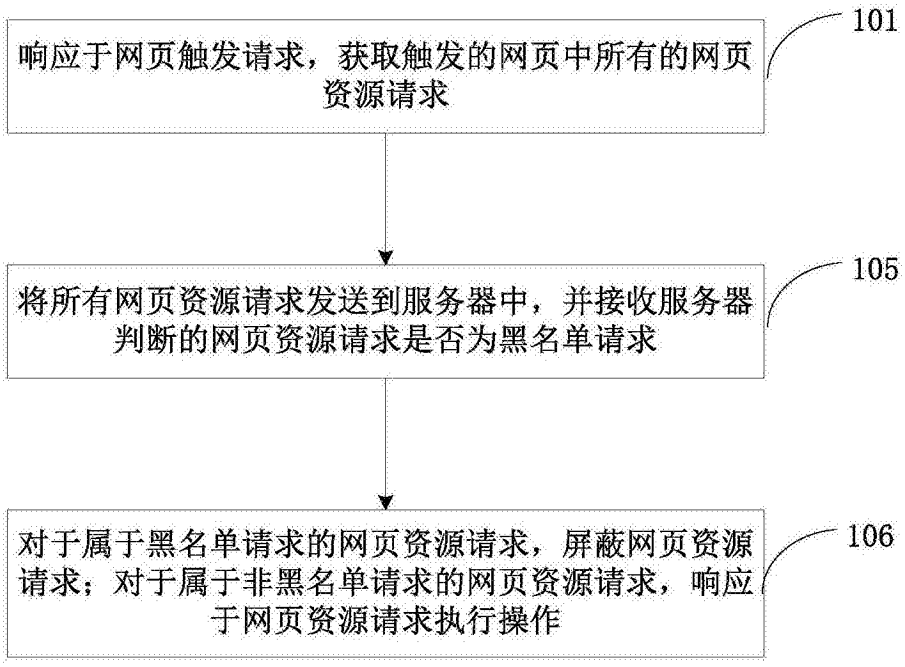

响应于网页触发请求，获取触发的网页中所有的网页资源请求
101
将所有网页资源请求发送到服务器中，并接收服务器判断的网页资源请求是否为黑名单请求
105
对于属于黑名单请求的网页资源请求，屏蔽网页资源请求；对于属于非黑名单请求的网页资源请求，响应于网页资源请求执行操作
106

图1

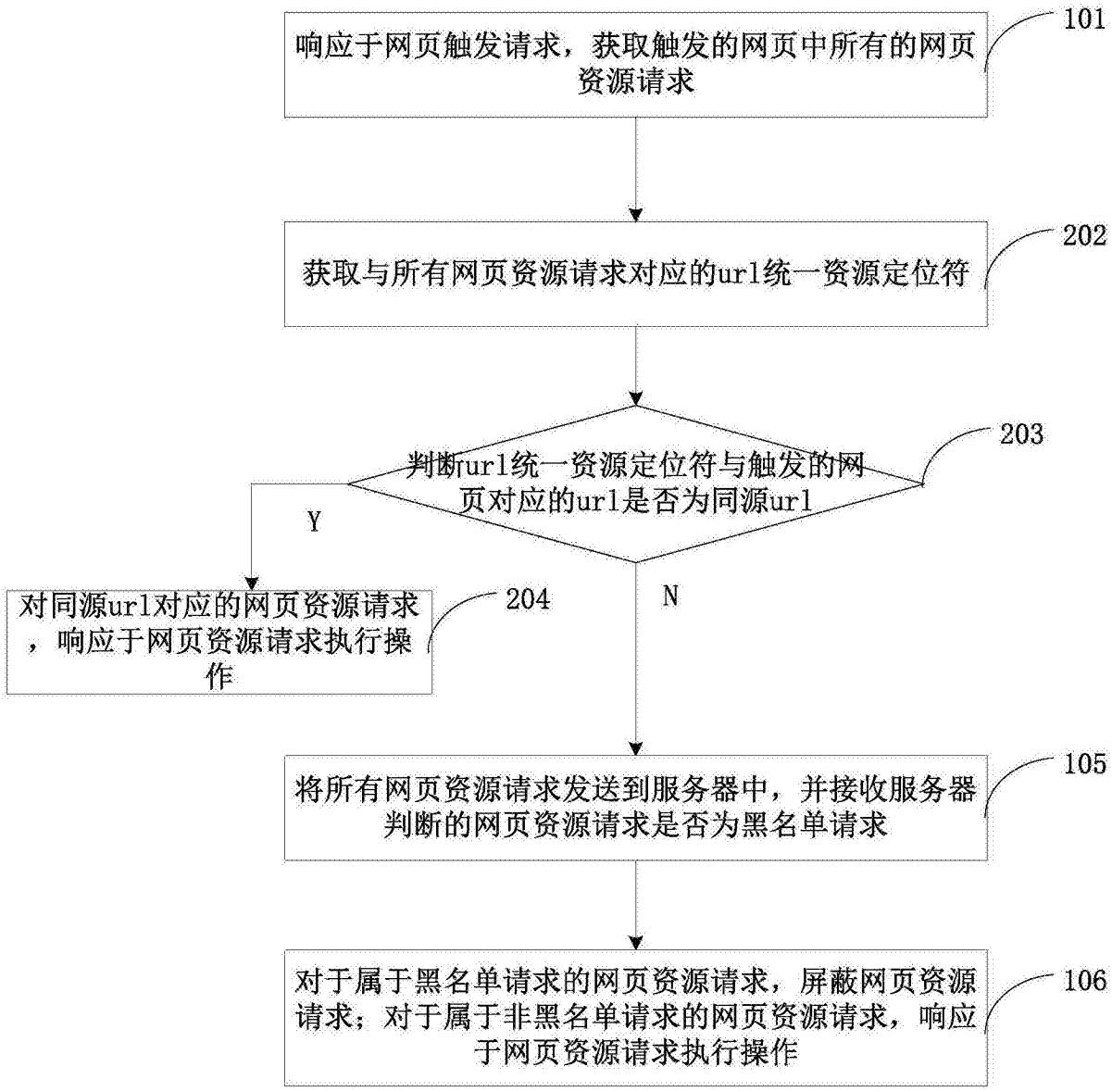

响应于网页触发请求，获取触发的网页中所有的网页资源请求
101
获取与所有网页资源请求对应的url统一资源定位符
202
判断url统一资源定位符与触发的网页对应的url是否为同源url
203
Y
N
对同源url对应的网页资源请求，响应于网页资源请求执行操作
204
将所有网页资源请求发送到服务器中，并接收服务器判断的网页资源请求是否为黑名单请求
105
对于属于黑名单请求的网页资源请求，屏蔽网页资源请求；对于属于非黑名单请求的网页资源请求，响应于网页资源请求执行操作
106

图2

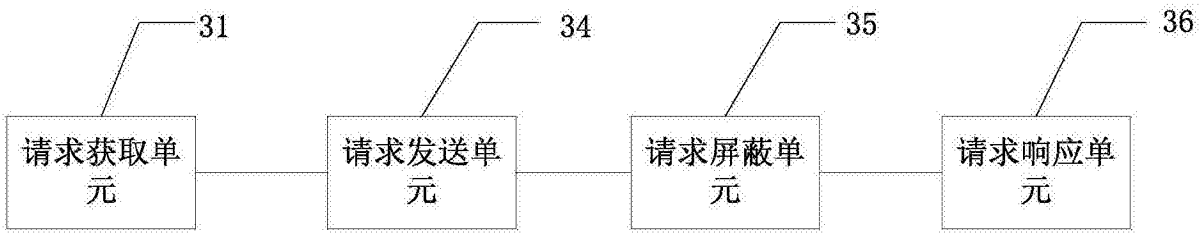

31
34
35
36
请求获取单元
请求发送单元
请求屏蔽单元
请求响应单元

图3

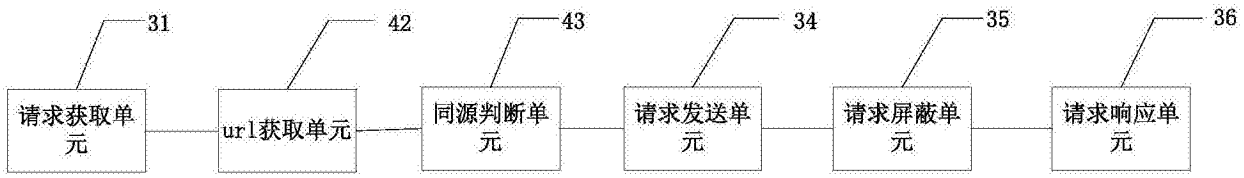

31
42
43
34
35
36
请求获取单元
url获取单元
同源判断单元
请求发送单元
请求屏蔽单元
请求响应单元

图4

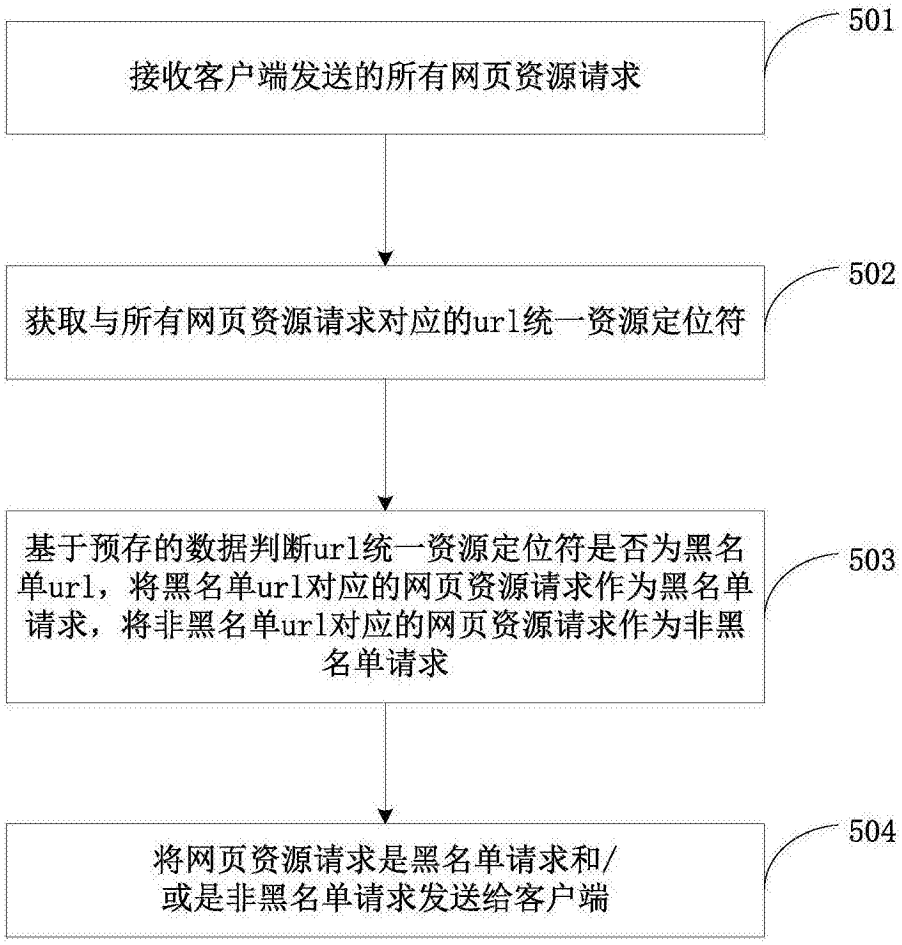

501
接收客户端发送的所有网页资源请求
502
获取与所有网页资源请求对应的url统一资源定位符
503
基于预存的数据判断url统一资源定位符是否为黑名单url，将黑名单url对应的网页资源请求作为黑名单请求，将非黑名单url对应的网页资源请求作为非黑名单请求
504
将网页资源请求是黑名单请求和/或是非黑名单请求发送给客户端

图5

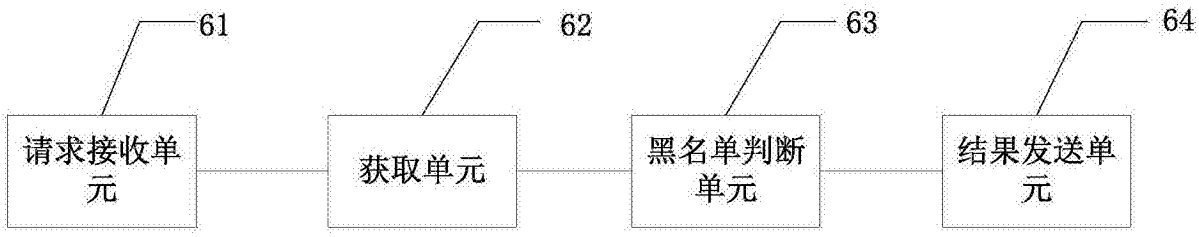

61
62
63
64
请求接收单元
获取单元
黑名单判断单元
结果发送单元

图6

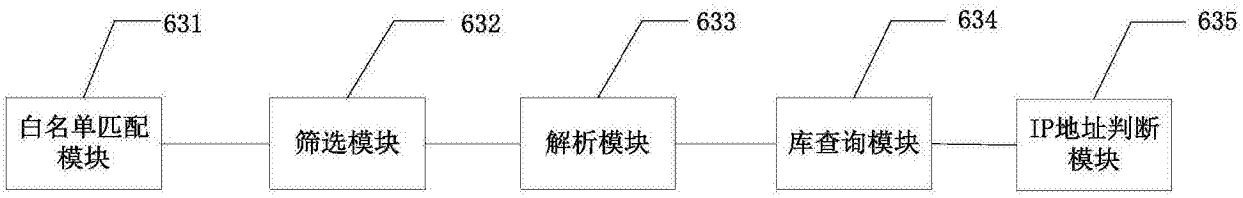


图7